UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

42640 7590 09/01/2009

DILLON & YUDELL LLP
8911 NORTH CAPITAL OF TEXAS HWY
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
SHIN, KYUNG H	
ART UNIT	**PAPER NUMBER**
2443	
MAIL DATE	**DELIVERY MODE**
09/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/651,548
Filing Date: August 29, 2000
Appellant(s): ATKINS ET AL.

Brian F. Russell
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5-22-09 appealing from the Office action mailed 12-24-08

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,807,277	**Doonan et al.**	10-2004
6,732,101	**Cook**	5-2004
4,888,800	**Marshall**	12-1999

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-29 are presented for examination. These rejections are set forth in prior Office Action, Paper No. 09/651,548\20081216 and reproduced for convenience.

Claim Rejection – 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1 - 4, 6 - 12, 14 - 20, 22 - 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doonan et al.** (US Patent No. **6,807,277**) in view of **Cook** (US Patent No. **6,732,101**).

Regarding Claims 1, 9, 17, Doonan discloses a network messaging system. (Doonan col 1, ll 10-12: *" … present invention is directed to a secure electronic messaging system …* ") Doonan discloses a method, a system and program product for managing a user key used to sign a message for a data processing system, the method comprising:

a) assigning a user key to a user and storing the user key in an encrypted data processing system utilized to encrypt messages; (Doonan col 2, ll 1-7: encryption key assigned by key server for message encryption)

b) encrypting the messages with the user key; (Doonan col 2, ll 7-8: message is encrypted)

c) storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein the associated key comprises a private key; (Doonan col 5, ll 63-67: generate an encrypted user key for transmission; col 5, ll 48-50: additionally; encrypted with a private key corresponding to digital certificate (private key used for information encryption; implies public key used for decryption)))

d) the encrypting data processing system communicating at least one encrypted messages together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; (Doonan col 6, l 1: encrypted message and encrypted key are transmitted to recipient)

f) a computer usable storage medium storing the control program. (Doonan col 3, ll 9-12; col 9, ll 33-44: software exists on computer readable medium for program execution)

Doonan discloses a check on the validation of a sender's credentials. (Doonan col 5, ll 16-20: sender credentials are verified) Doonan does not explicitly disclose revoking the associated key at the encrypting data processing system to prevent validation.

However, Cook discloses:

e) preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key. (Cook col 6, ll 40-50: association key deleted (revoked: see spec. page 15 lines 27-28: "Associated key A may be **revoked by simply erasing it** from server system 104.") as per specification by software component at the user system software component residing (data encryption system))

The specification discloses the procedure to prevent validation of the association key such as by revoking an associated key. Cook discloses an equivalent procedure for revoking or erasing or deleing the associated key.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to delete (revoke) an association key and prevent validation of the association of the user as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38: " … *Messages can be encrypted using any available encryption means at the sender and sent to a forwarding service. The forwarding service can forward the message to each recipient according to the recipient's decryption capability and preference.* … ")

Regarding Claims 2, 10, 18, Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (Doonan col 6, ll 1-3: encrypted key is decrypted)

b) decrypting the messages with the user key. (Doonan col 6, ll 1-3: encrypted message is decrypted)

Regarding Claims 3, 11, 19, Doonan discloses the method, system and program product according to Claims 1, 9, 17, wherein: the encrypting data processing system further comprises a client system and a server system coupled for communication, the client system (Doonan col 3, ll 9-12: network connected client (sender) and server system) having a client memory device and the server system having an encryption chip and a server memory device:

a) storing the user key further comprises storing the user key in the client memory device; (Doonan col 9, ll 44-47: memory area used for data and workspace storage)

b) storing the associated key further comprises storing the associated key in the server memory device; (Doonan col 5, ll 4-5: key is stored at server system database)

Doonan discloses a check on the validation of a sender's credentials. (Doonan col 5, ll 16-20: sender credentials are verified) Doonan does not explicitly disclose preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

However, Cook discloses:

c) preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device. (Cook col 6, ll 40-50: deletion (revocation) of association key at system via software component on server system in order to prevent validation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to prevent validation of messages associated with the user by eliminating the associated key as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38)

Regarding Claims 4, 12, 20, Doonan does not explicitly disclose a server system to receive, encryption and forward message. However, Cook discloses the method, system and program product according to Claims 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server system; (Cook col 2, ll 19-23: send message from client to server for encryption)
b) encrypting the messages using the encryption chip of the server system; (Cook col 2, ll 51-55: encrypt message)
c) sending the encrypted messages from the server system to the client system. (Cook col 2, ll 51-55: deliver encrypted message to recipient (client) system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to send messages, encrypt messages, and retrieve encrypted messages as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (Cook col 2, ll 33-38)

Regarding Claims 6, 14, 22, Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising: encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system. (Doonan col 2, ll 3-8: encryption key transferred to sender system)

Regarding Claims 7, 15, 23, Doonan discloses the method, system and program product according to Claims 6, 14, 22, further comprising:
communicating an encrypted associated key to validate the association of the user with the encrypted messages. (Doonan col 5, ll 63-67)

Regarding Claims 8, 16, 24, Doonan discloses the method, system and program product according to Claims 7, 15, 23, further comprising: decrypting the associated key with the encryption chip key. (Doonan col 6, ll 1-3)

3. **Claims 5, 13, 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doonan-Cook** and further in view of **Marshall** (US Patent No. **4,888,800**).

Regarding Claims 5, 13, 21, Doonan-Cook does not explicitly disclose the ability to erase key information after processing of an encrypt message. However, Marshall discloses the method, system and program product according to Claims 4, 12, 20, further comprising: erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (Marshall col 2, ll 30-35: key information is erased from system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan-Cook to erase all key related information after message processing maintaining only current information as taught by Marshall. One of ordinary skill in the art would be motivated to employ Marshall in order to enable a flexible and strengthened network key management system. (Marshall col 1, ll 50-58: " … *system has the advantage … only to maintain the keys required for whatever current communication sessions … a pair of session keys … every time a link or session is requested* … ")

(10) Response to Argument

(I) Claims 17-24 are rejected under 35 U.S.C. § 101 as non-statutory;

Response to **(I)**:

The 101 rejection has been withdrawn based on remarks from Applicant.

(II) Claims 1-4, 6-12, 14-20 and 22-24 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,807,277 to Doonan et al. (Doonan) in view of U.S. Patent No. 6,732,101 to Cook;

A1.: Applicant argues *"associated key comprises a private key". (Appeal Remarks Page 11)*

Response to A1:

Applicant amended claim limitation such that the associated key is explicitly a private key. There is no explicit disclosure in the specification or original claims for the associated key to be a private key.

Doonan discloses that an equivalent associated key is encrypted using a public key. Doonan also discloses in different encryption procedures that a private key within a public/private key pair can be used to encrypt information such as a message or a key. (Doonan col 5, ll 63-67: generate an encrypted user key for transmission; col 5, ll 48-50: additionally; encrypted with a private key corresponding to digital certificate (private key used for information encryption; implies public key used for decryption)) This encryption process is equivalent to Applicant's claim limitation of an encryption process using a private key. A private key can also be used to encrypt data. Doonan discloses a private key used as an encryption key used for an encryption process.

The capability is well known in the art for one key (i.e. public or private) to be used for encryption and the other key (i.e. public or private) to be used for decryption.

A2: Applicant argues *preventing validation. (Appeal Remarks Page 13)*

Response to **A**2:

The claim limitation states, *"preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able* *to decrypt the encrypted user key"*. The claim limitation states a cause and effect situation. In order to prevent validation of the association of the user with messages, the associated key is revoked.

In other words, the claim limitation discloses how to *"preventing validation of the association of the user with messages"*. The action to prevent this is "by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key".

The specification discloses the procedure used to revoke an associated key. The association key is deleted (i.e. erased) or revoked as per specification by a software component at the user system software component or data encryption system. (The revoked definition: see Spec. Page 15, ll 27-28: "Associated key A may be **revoked by simply erasing it** from server system 104.")

Specification Page 15, lines 17-33:
Method 300 then proceeds to block 320. Block 320 illustrates that if revocation of user key 1 for user 1 is desired (e.g., user 1 is no longer employed at the company maintaining data processing system i00 and validation of user key 1 needs to be revoked), then validation of encrypted, hashed messages associated with user 1 can be prevented by revoking associated key A on server system 104. Associated keys, such as associated keys A, B, and C, are never used outside of server system 104 and are generally only accessed and managed by an authorized system administrator. **Associated key A may be revoked by simply erasing it from server system 104**. Since associated key A is revoked and no longer exists in server system 104, then ECK 107 does not have an associated key to decrypt, and encrypted user key 1, in turn, cannot be decrypted since associated key A does not exist to decrypt user key 1. Method 300 finally ends at block 322.

The claimed invention does not address the fact that *"the simple deletion at the sender (i.e., encrypting) system of a message recipient's public key"* does not *"prevent validation of the association of the user with messages"* and does not render the encrypting data processing system unable *"to decrypt the encrypted user key"*. This argued claim limitation and statement is not addressed in the claimed invention.

Cook discloses an equivalent procedure, which is the erasure of a key, in order to revoke an associated key. (Cook col 6, ll 40-50: encryption key deleted)

The claim limitation states the procedure to be completed in order revoke an associated key. Revoking of the association key prevents validation of the association of the user with messages.

B: Applicant argues *dependent claims. (Appeal Remarks Page 14)*

Response to **B**:

The successful responses to arguments for independent claims also respond to the current arguments against the dependent claims.

C: Applicant argues *an encryption chip. (see Appeal Remarks Page 14)*

Response to **C**:

This is the first time this argument has been presented by Applicant. Doonan discloses a computer system utilizing data encryption. Doonan discloses the utilization of a special purpose computer utilizing firmware such as an Integrated Circuit (IC). This particular IC is used to perform encryption functions. (Doonan col 9, ll 32-39: special purpose computers; store firmware and executable software code)

(III) Claims 5, 13 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over Doonan and Cook in view of U.S. Patent No. 4,888,800 to Marshall.

Applicant argues *dependent claims. (Appeal Remarks Page 16)*

Response to **(III)**:

The successful responses to arguments for independent claims also respond to the current arguments against the dependent claims.

(11) Related Proceeding(s) Appendix

Copies of the court or Board decision(s) identified in the Related Appeals and Interferences section of this examiner's answer are provided herein.

Appeal No. 2006-2482; Decision on Appeal mailed April 5, 2007

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Kyung Hye Shin/

Examiner, Art Unit 2443

Conferees:

/J Bret Dennison/

Primary Examiner, Art Unit 2443

/Tonia LM Dollinger/
Supervisory Patent Examiner, Art Unit 2443